PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-208965
(43)Date of publication of application : 26.07.2002

(51)Int.Cl. H04L 12/66
G06F 13/00
G06F 15/00
H04L 9/32

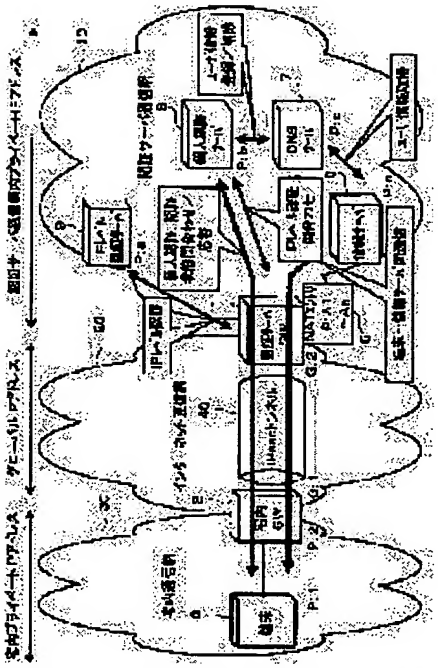
(21)Application number : 2001-000062
(22)Date of filing : 04.01.2001

(71)Applicant : NEC CORP
NTT COMMUNICATIONS KK

(72)Inventor : KANO OSAMU
INOUE TAKUYA
MIZOGUCHI YOICHI

(54) INTERNET RELAY CONNECTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To achieve high level security at the time of authenticating a terminal connected from a home communication network to the Internet by dial-up, and an IP address is assigned according to the connection.
SOLUTION: An IP sec tunnel is set in a communication path in the Internet communication network so that the secured communication can be performed through the IPsec tunnel between a home communication network and an authentication server communication network. Moreover, authentication strength can be enhanced by the two stages of the IP level authentication of the IPsec tunnel establishment and the personal identification of an information server access, and a consumer can be specified from the IP address according to the linkage of an authentication server GW, an IP level authentication server, and a personal identification server. The consumer information can be acquired from the access IP address by an information server.



LEGAL STATUS

[Date of request for examination]	01.02.2002
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3616570
[Date of registration]	12.11.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－208965
（P2002－208965A）
(43)公開日　平成14年７月26日(2002.7.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ	５Ｂ０８５
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
15/00	３３０	15/00	３３０Ｂ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｋ０３０

審査請求　有　　請求項の数12　ＯＬ　（全９頁）

(21)出願番号　特願2001－62(P2001－62)

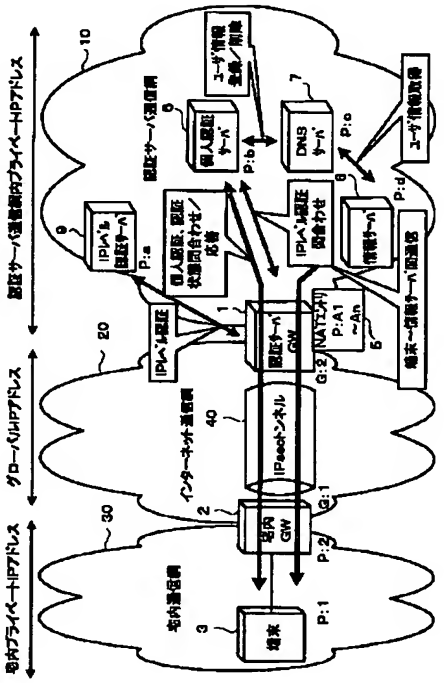
(22)出願日　平成13年１月４日(2001.1.4)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　加納　修
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100078237
弁理士　井出　直孝　（外１名）

最終頁に続く

(54)【発明の名称】　インターネット中継接続方式

(57)【要約】
【課題】　宅内通信網からダイアルアップによりインターネットに接続され、接続によりＩＰアドレスがアサインされる端末の認証について、そのセキュリティを高度化する。
【解決手段】　インターネット通信網内の通信路にＩＰｓｅｃトンネルを設定し、宅内通信網と認証サーバ通信網との間にＩＰｓｅｃトンネルによるセキュアな通信を可能とする。さらに、ＩＰｓｅｃトンネル確立のＩＰレベル認証と情報サーバアクセスの個人認証の二段階により、認証強度を高め、認証サーバＧＷ、ＩＰレベル認証サーバ、個人認証サーバの連携により、ＩＰアドレスからコンシューマを特定し、情報サーバはアクセスしてきたＩＰアドレスからコンシューマ情報を取得する。



1

【特許請求の範囲】

【請求項１】　ダイアルアップによりインターネット・プロトコル（ＩＰ，internet protocol）に準拠するアドレスが付与され、端末を含む宅内通信網とグローバルアドレスによりインターネット・プロトコルに基づく通信を行うインターネット通信網との接続点に設けられた宅内ＧＷ（Gate Way）と、

複数の認証サーバを含みインターネット・プロトコルに準拠するプライベートＩＰアドレスにより制御される認証サーバ通信網（ＣＳＮ，Certified Server Network）と前記インターネット通信網との接続点に設けられた認証サーバＧＷ（Gate Way）とを備えたインターネット中継接続方式において、

前記インターネット通信網の中に前記宅内ＧＷと前記認証サーバＧＷとの間に、ＩＰｓｅｃ（internet protocol security）トンネルを設定する手段を備えたことを特徴とするインターネット中継接続方式。

【請求項２】　前記ＩＰｓｅｃトンネルはＯＳＩ（open system interconnection)第３層に設定された暗号化通信方式により構築された請求項１記載のインターネット中継接続方式。

【請求項３】　前記認証サーバＧＷは、多数のプライベートＩＰアドレスをプールしておくＮＡＴ（network address translator）手段と、前記トンネルが設定されたときにそのＮＡＴ手段にプールしてあるプライベートＩＰアドレスを通信に関わる前記宅内通信網に属する端末に割り振る手段と、前記端末から到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって対応する認証サーバ通信網内のサーバにルーティングする手段と、前記認証サーバ通信網内のサーバから到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって前記ＩＰｓｅｃトンネルを介して対応する端末にルーティングする手段とを含む請求項２記載のインターネット中継接続方式。

【請求項４】　前記認証サーバ通信網の中に、個人認証を行う個人認証サーバおよびドメイン名の管理を行うＤＮＳ（domain name system）サーバを少なくとも一つずつ含み、前記個人認証サーバは個人認証を実行した端末のユーザ情報を前記ＤＮＳサーバに引き渡す手段を備え、前記ＤＮＳサーバはそのユーザ情報を登録する手段を備えた請求項３記載のインターネット中継接続方式。

【請求項５】　前記登録する手段には、ユーザ識別子（ＩＤ）、認証の有効期限、およびサービス・カテゴリの情報を登録する手段を含む請求項４記載のインターネット中継接続方式。

【請求項６】　前記認証サーバ通信網内にある一つの情報サーバが前記端末の一つからアクセスを受けたときに、前記ＤＮＳサーバに対してその端末に割り振られた前記プライベートＩＰアドレスをキーとして問い合わせを行う手段と、この問い合わせに対して前記個人認証サーバに登録されたその端末に関する情報をその問い合わせを行った情報サーバに渡す手段とを備えた請求項５記載のインターネット中継接続方式。

2

【請求項７】　前記個人認証サーバは、前記ＤＮＳサーバに対し、個人認証状態を終了した端末に関する情報を削除する要求を行う手段を含み、

前記ＤＮＳサーバは、当該要求にしたがって該当する情報を削除する手段を含む請求項６記載のインターネット中継接続方式。

【請求項８】　前記端末には、前記個人認証サーバからの認証の通知に対応して認証中を意味する表示をその端末の表示装置に表示する手段を含む請求項４記載のインターネット中継接続方式。

【請求項９】　前記端末には前記個人認証サーバに対して認証状態の問い合わせを行う手段を備え、前記個人認証サーバにはこの問い合わせに対して認証状態を応答する手段を備えた請求項８記載のインターネット中継接続方式。

【請求項１０】　前記個人認証サーバには、認証中にある端末について前記認証状態の問い合わせがあったときにはその問い合わせから所定時間だけその認証状態を維持する手段を含む請求項９記載のインターネット中継接続方式。

【請求項１１】　前記個人認証サーバには、認証中にある端末から認証終了の要求を受けたときにその認証状態を終了させる手段を備えた請求項９記載のインターネット中継接続方式。

【請求項１２】　前記認証サーバＧＷには、一つの端末からＨＴＴＰ（hypertext transfer protocol)によるアクセスがあったときにその端末の個人認証が未認証であるときにはその端末を認証を促すための認証ページに誘導する手段を備えた請求項４記載のインターネット中継接続方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、宅内通信網内のダイアルアップ環境下にある端末と、認証サーバ通信網内にあり情報提供源となる情報サーバとが、インターネットを介して接続するための中継接続に利用する。本発明は、ＩＰ（internet protocol）による通信のセキュリティ（ＩＰｓｅｃ，internet protocol security）を高度化する技術に関する。本発明は、異なるネットワーク間のアドレス変換（ＮＡＴ，network address translation）に関する。

【０００２】

【従来の技術】インターネットの普及により、インターネットを利用したビジネスやサービスが加速度的に増加し、盗聴や「なりすまし」などを防止する通信のセキュリティがきわめて重要になっている。高度のセキュリティを行うために通信相手の正当性を確認するための認証

および他人に通信を盗聴されないための暗号化などがさまざまに利用されている。

【０００３】このために、インターネットおよびＩＳＰ(internet service provider)を経由した端末と情報サーバ間に高度のセキュリティを維持して通信を行う、ＳＳＬ(secure sockets layer)が知られている。ＳＳＬは国際標準化機構（ＩＳＯ）に定められたＯＳＩ(open system interconnection)第５層にあたるプロトコルである。

【０００４】

【発明が解決しようとする課題】近年、宅内通信網からダイアルアップ接続によりインターネットを経由して、情報提供その他のサービスを受けることができるようになった。そして宅内通信網内の端末には、インターネット・プロトコルによるアドレスが固定的に付与されず、その端末がダイアルアップにより接続されたときにインターネット・プロトコルによるアドレスがアサインされ、その接続が終了したときには、そのアドレスはまた他の端末にアサインされるようにして利用されるものが普及することになった。

【０００５】そのようなアドレスについては、そのアドレスをキーとしてセキュリティを設定すると、かりにインターネット網の中で接続の終了および再接続が行われることがあると、その宅内通信網に無関係の端末による「なりすまし」が可能になる。すなわち宅内通信網内の端末がインターネットを介して認証サーバにアクセスする場合に、従来のセキュリティに加えて宅内通信網の外部からの侵入を防ぐためのセキュリティの強化が必要である。

【０００６】本発明は、このような背景に行われたものであって、宅内通信網からダイアルアップ接続によりインターネットを経由して、認証サーバにアクセスする通信接続に対して、インターネット網内のセキュリティを強化する中継接続方式を提供することを目的とする。本発明は、このようなセキュリティを強化するとともに、認証の強度を上げることができる中継接続方式を提供することを目的とする。本発明は、さらに情報サーバがアクセスを受け付けた認証サーバ通信網内プライベートＩＰアドレスからユーザ情報の取得を可能とする中継接続方式を提供することにより、一度認証を行えば、認証サーバ通信網内サーバ間で、その認証情報を共有することが可能となり、ユーザはサービス提供のたびに認証情報通信の必要がない、いわゆるＳＳＯ(Single Sign On)サービスを提供することを目的とする。本発明は、端末が認証状態を把握することを可能とする中継接続方式を提供することを目的とする。本発明は、認証状態を必要な期間維持することができる中継接続方式を提供することを目的とする。本発明は、個人未認証の場合に個人認証を促すことができる中継通信方式を提供することを目的とする。本発明は、ＩＰレベル認証の対象と個人認証の対象を管理することができる中継接続方式を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明は、ダイアルアップによりインターネット・プロトコル（ＩＰ, internet protocol）に準拠するアドレスが付与され、端末を含む宅内通信網とグローバルアドレスによりインターネット・プロトコルに基づく通信を行うインターネット通信網との接続点に設けられた宅内ＧＷ（Gate Way）と、複数の認証サーバを含みインターネット・プロトコルに準拠するプライベートＩＰアドレスにより制御される認証サーバ通信網（ＣＳＮ, Certified Server Network）と前記インターネット通信網との接続点に設けられた認証サーバＧＷ（Gate Way）とを備えたインターネット中継接続方式において、前記インターネット通信網の中に前記宅内ＧＷと前記認証サーバＧＷとの間に、ＩＰｓｅｃ（internet protocol security）トンネルを設定する手段を備えたことを特徴とする。

【０００８】前記ＩＰｓｅｃトンネルはＯＳＩ（open system interconnection)第３層に設定された暗号化通信方式により構築することができる。このＩＰｓｅｃはＯＳＩ第３層レベルでの暗号化通信方式を利用することにより、ＩＰ上のアプリケーションであれば全てのサービスを提供することが可能になる。

【０００９】また、ＶＰＮ(Virtual Private Network：仮想施設網)は主に企業の拠点間通信に用いられるが、宅内通信網と認証サーバ通信網との間にＩＰｓｅｃトンネルを構築することにより、認証サーバ通信網内のサーバと不特定多数の宅内通信網内の端末とのＩＰ－ＶＰＮによるセキュアな通信を可能とする。

【００１０】さらに、ＩＰｓｅｃトンネル確立のＩＰレベル認証と情報サーバアクセスの個人認証のレイヤの違う認証システムを連携することによりスムースなサービス提供を可能とする。すなわち、認証サーバＧＷ、ＩＰレベル認証サーバ、個人認証サーバの連携により、ＩＰアドレスからユーザを特定し、情報サーバはアクセスしてきたＩＰアドレスからユーザ情報を取得することができるようになる。

【００１１】すなわち、本発明は、端末と情報サーバ間の異レイヤ間認証連携によるスムースなエンドツーエンド(end to end)通信における端末と情報サーバとの間の通信を行うためのアドレス割当技術、ＩＰレベル認証と個人認証が連携した認証技術、認証サーバＧＷのＮＡＴ機能での個人認証状態の管理技術、情報サーバがアクセスしたユーザ情報の取得技術、ならびに端末に情報サーバへアクセスが可能であるかどうかの認証状態の表示技術を提供する。また、一度の認証で複数のサービスを利用できるＳＳＯサービスをアプリケーションプロトコルに依存せず、ＩＰレイヤレベルで実現する。

【００１２】前記認証サーバＧＷは、多数のプライベー

トＩＰアドレスをプールしておくＮＡＴ（network address translator）手段と、ＩＰｓｅｃトンネルが設定されたときにそのＮＡＴ手段にプールしてあるプライベートＩＰアドレスを通信に関わる前記宅内通信網に属する端末に割り振る手段と、前記端末から到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって対応する認証サーバ通信網内のサーバにルーティングする手段と、前記認証サーバ網内のサーバから到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって前記ＩＰｓｅｃトンネルを介して対応する端末にルーティングする手段とを含むことが望ましい。

【００１３】前記認証サーバ通信網の中に、個人認証を行う個人認証サーバおよびドメイン名の管理を行うＤＮＳ（domain name system）サーバを少なくとも一つずつ含み、前記個人認証サーバは個人認証を実行した端末のユーザ情報を前記ＤＮＳサーバに引き渡す手段を備え、前記ＤＮＳサーバはそのユーザ情報を登録する手段を備えることが望ましい。

【００１４】前記登録する手段には、ユーザ識別子（ＩＤ）、認証の有効期限、およびサービス・カテゴリの情報を登録する手段を含むことが望ましい。

【００１５】前記認証サーバ通信網（ＣＳＮ）内にある一つの情報サーバが前記端末の一つからアクセスを受けたときに、前記ＤＮＳサーバに対してその端末に割り振られた前記プライベートＩＰアドレスをキーとして問い合わせを行う手段と、この問い合わせに対して前記個人認証サーバに登録されたその端末に関する情報をその問い合わせを行った情報サーバに渡す手段とを備えることが望ましい。

【００１６】前記個人認証サーバは、前記ＤＮＳサーバに、個人認証状態を終了した端末に関する情報を削除する要求を行う手段を含み、前記ＤＮＳサーバは、当該要求にしたがって該当する情報を削除する手段を含むことが望ましい。

【００１７】前記端末には、前記個人認証サーバからの認証の通知に対応して認証中を意味する表示をその端末の表示装置に表示する手段を含むことが望ましい。

【００１８】前記端末には前記個人認証サーバに対して認証状態の問い合わせを行う手段を備え、前記個人認証サーバにはこの問い合わせに対して認証状態を応答する手段を備えることが望ましい。

【００１９】前記個人認証サーバには、認証中にある端末について前記認証状態の問い合わせがあったときにはその問い合わせから所定時間だけその認証状態を維持する手段を含むことが望ましい。

【００２０】前記個人認証サーバには、認証中にある端末から認証終了の要求を受けたときにその認証状態を終了させる手段を備えることが望ましい。

【００２１】前記認証サーバＧＷには、一つの端末からＨＴＴＰによるアクセスがあったときにその端末の個人認証が未認証であるときにはその端末を認証を促すための認証ページに誘導する手段を備えることが望ましい。

【００２２】

【発明の実施の形態】本発明実施例のインターネット中継接続方式の構成を図１を参照して説明する。図１は本発明実施例のインターネット中継接続方式の全体構成図である。

【００２３】本発明は、図１に示すように、ダイアルアップによりインターネット・プロトコルに準拠するアドレスが付与され、端末３を含むインターネット・プロトコルに準拠するプライベートＩＰアドレスにより制御される宅内通信網３０とグローバルアドレスによりインターネット・プロトコルに基づく通信を行うインターネット通信網２０との接続点に設けられた宅内ＧＷ２と、複数の認証サーバを含みインターネット・プロトコルに準拠するプライベートＩＰアドレスにより制御される認証サーバ通信網１０とインターネット通信網２０との接続点に設けられた認証サーバＧＷ１とを備えたインターネット中継接続方式である。

【００２４】ここで、本発明の特徴とするところは、インターネット通信網２０の中に宅内ＧＷ２と認証サーバＧＷ１との間に、ＩＰｓｅｃトンネル４０を設定するところにある。本発明実施例のインターネット中継接続方式の特徴を以下に列挙する。

【００２５】認証サーバＧＷ１は、多数のプライベートＩＰアドレスをプールしておくＮＡＴ機能５を備え、ＩＰｓｅｃトンネル４０が設定されたときにそのＮＡＴ機能５にプールしてあるプライベートＩＰアドレスを通信に関わる宅内通信網３０に属する端末３に割り振り、端末３から到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって対応する認証サーバ通信網１０内の各サーバにルーティングし、認証サーバ通信網１０内の各サーバから到来する通信パケットをその通信パケット内の宛て先アドレスにしたがってＩＰｓｅｃトンネル４０を介して対応する端末にルーティングする。

【００２６】認証サーバ通信網１０の中に、個人認証を行う個人認証サーバ６およびドメイン名の管理を行うＤＮＳ（domain name system）サーバ７を少なくとも一つずつ含み、個人認証サーバ６は個人認証を実行した端末のユーザ情報をＤＮＳサーバ７に引き渡し、ＤＮＳサーバ７はそのユーザ情報を登録する。この登録には、ユーザ識別子（ＩＤ）、認証の有効期限、およびサービス・カテゴリの情報を登録する。

【００２７】ＩＰレベル認証により正当性が認証されると、ＩＰｓｅｃトンネル４０を確立し、その後個人認証サーバ６により個人認証を行う。個人認証サーバ６はＮＡＴ機能５により割り振られたプライベートＩＰアドレスであるアクセス元（発）ＩＰアドレスをキーに認証サーバＧＷ１にＩＰレベル認証のユーザを問い合わせる。個人認証サーバ６は、その問い合わせ結果と自分で保持

している個人認証情報からＩＰレベル認証と個人認証間の整合性のチェックを行い、問題なければ個人認証の正当性を認証する。また、ＤＮＳサーバ７に対してアクセス元（発）ＩＰアドレスをキーとしてドメインにユーザＩＤ、有効期限等のユーザ情報を適用しＤＮＳの登録を行い、その後、ユーザからアクセスがあった情報サーバはアクセス元（発）ＩＰアドレスをキーにＤＮＳサーバに問い合わせを行い、その応答としてユーザ情報を含むドメイン名を取得する。

【００２８】個人認証サーバ６は、ＤＮＳサーバ７に、個人認証状態を終了した端末３に関する情報を削除する要求を行い、ＤＮＳサーバ７は、この要求にしたがって該当する情報を削除する。

【００２９】端末３には、個人認証サーバ６からの認証の通知に対応して認証中を意味する表示をその端末３の表示装置に表示する。

【００３０】端末３は個人認証サーバ６に対して認証状態の問い合わせを行い、個人認証サーバ６にはこの問い合わせに対して認証状態を応答する。

【００３１】個人認証サーバ６には、認証中にある端末３について前記認証状態の問い合わせがあったときにはその問い合わせから所定時間だけその認証状態を維持する。

【００３２】個人認証サーバ６は、認証中にある端末３から認証終了の要求を受けたときにその認証状態を終了させる。

【００３３】認証サーバＧＷ１は、一つの端末３からＨＴＴＰによるアクセスがあったときにその端末３の個人認証が未認証であるときにはその端末３に認証を促すために、その端末３を個人認証サーバ上の認証ページに誘導する。

【００３４】図１に示すネットワーク構成例を参照して本発明のインターネット中継接続方式の特徴的なシーケンスを簡単に説明すると、端末３にプライベートＩＰアドレスを付与する。端末３はダイヤルアップ環境でインターネットまたはＩＳＰ（internet service provider）を経由して認証サーバＧＷ１へ接続を要求する。ＩＰレベル認証サーバ９は宅内ＧＷ２を認証し、認証が認められると宅内ＧＷ２と認証サーバＧＷ１との間でＩＰｓｅｃトンネル４０を確立する。認証サーバＧＷ１はインターネットまたはＩＳＰを経由して接続する端末３を認証サーバ通信網１０でユニークに扱うためにＮＡＴ機能５を有する。ＮＡＴ機能５で使用するＮＡＴエントリテーブルにおいて端末３の個人認証状態を管理する。宅内通信網３０、認証サーバ通信網１０内はプライベートＩＰアドレスにより通信を行い、端末３からの認証サーバ通信網１０へアクセスが発生するとプライベートＩＰアドレスを端末３に割り当てる。ＩＰレベル認証を行った後、個人認証サーバ６はユーザの個人認証を行う。個人認証サーバ６は、アクセスしたプライベートＩＰアドレスからＩＰレベル認証を行った宅内ＧＷ２の識別情報を認証サーバＧＷ１から取得しＩＰレベル認証と個人認証の関係の正当性をチェックする。ＩＰレベル認証、個人認証を行うとＩＰレベル認証サーバ９と個人認証サーバ６は連携しＤＮＳサーバ７にアクセスしたユーザ情報を登録し、情報サーバ８はＤＮＳサーバ７に問い合わせを行い、ユーザ情報を取得する。個人認証サーバ６は個人認証の状態を端末３へ通知し、端末３は個人認証サーバ６へ認証状態の問い合わせを行う。認証サーバＧＷ１は、個人認証を行っていない場合には、個人認証サーバ６に個人認証を促す。

【００３５】以下、本発明実施例をさらに詳細に説明する。図１を参照して、本実施例は宅内通信網３０内の端末３、宅内ＧＷ２、認証サーバ通信網１０内の認証サーバＧＷ１、ＩＰレベル認証サーバ９、個人認証サーバ６、ＤＮＳサーバ７、情報サーバ８を含む。

【００３６】ユーザは端末３を操作して宅内ＧＷ２を介しダイヤルアップ接続によりインターネットまたはＩＳＰ（internet service provider)を経由して認証サーバ通信網１０に接続する。認証サーバＧＷ１は、宅内ＧＷ２との間でＩＰｓｅｃトンネル４０を確立する。認証サーバＧＷ１はＮＡＴ機能５を有し、また端末３を認証サーバ通信網１０内でユニークと扱うためのプライベートＩＰアドレスをプールする。ＩＰレベル認証サーバ９は、認証サーバＧＷ１からの認証要求に対し端末３とＩＰｓｅｃトンネル４０の確立を行うための認証を行う。個人認証サーバ６は、ＩＰレベル認証を行った後ユーザ個人を認証する。ＤＮＳサーバ７は、ユーザ情報を保持する。ユーザ情報は、ＩＰレベル認証サーバ９と個人認証サーバ６が連携し認証を行うと登録し、認証が終了すると削除する。情報サーバ８は認証サーバ通信網１０に接続したユーザの端末３に情報を提供する。情報サーバ８はアクセスのあった端末３にＮＡＴ機能５により割り振られたプライベートＩＰアドレスをＤＮＳサーバ７に問い合わせ、ユーザ情報を取得する。

【００３７】次に、図１ないし図５を参照して本実施例の動作について詳細に説明する。図２は宅内ＧＷ２と認証サーバＧＷ１との間に確立されたＩＰｓｅｃトンネルの概念図である。図３は異なるネットワーク間を転送されるパケットのアドレス付与状況を示す図である。図４は個人認証サーバ、ＤＮＳサーバ、情報サーバ相互間の動作を示す図である。図５は本発明実施例のインターネット中継接続方式の全体的な動作を示す図である。

【００３８】宅内ＧＷ２は、ユーザが操作する端末３にプライベートＩＰアドレスを割り振り、ダイヤルアップ接続によりＩＳＰよりグローバルＩＰアドレスが割り振られる。認証サーバＧＷ１は、端末３とのＩＰｓｅｃトンネル通信で使用するグローバルＩＰアドレスと宅内の端末３を認証サーバ通信網１０内でユニークに扱うためプライベートアドレスをプールする。宅内ＧＷ２はユー

ザの端末３からの認証サーバ通信網１０内の情報サーバ８へのアクセスを検出すると、宅内ＧＷ２と認証サーバＧＷ１間にグローバルＩＰアドレスを使用したＩＰｓｅｃトンネル４０の確立を要求する。

【００３９】認証サーバＧＷ１は宅内ＧＷ２とＩＰｓｅｃトンネル４０の接続可否を、ＩＰレベル認証サーバ９に問い合わせる。ＩＰレベル認証サーバ９は、宅内ＧＷ２の認証を行い、宅内ＧＷ２と認証サーバＧＷ１との間のＩＰｓｅｃトンネル４０の確立可否を応答する。確立可の場合には宅内ＧＷ２と認証サーバＧＷ１との間でグローバルＩＰアドレスを使用したＩＰｓｅｃトンネル４０を確立する。

【００４０】ＩＰｓｅｃトンネル４０を確立すると、プールしてある認証サーバ通信網１０内のプライベートＩＰアドレスを割り振る。認証サーバＧＷ１は、ＮＡＴ機能５により図のように認証サーバ通信網１０内のプライベートＩＰアドレスを管理することでユーザの端末３を認証サーバ通信網１０内でユニークとする。ＮＡＴ機能５ではＩＰｓｅｃ確立要求を受け付けた各端末毎に個人認証状態を管理する。

【００４１】ＮＡＴ機能５のＮＡＴエントリ情報で管理している個人認証状態が個人認証未である場合には、個人認証サーバ６の個人認証ページに誘導することで個人認証をユーザに促す。

【００４２】その個人認証サーバ６は、認証サーバＧＷ１と連携してＩＰレベル認証の識別情報と個人認証の識別情報の組み合わせ関係の正当性をチェックし、ユーザに割り振った認証サーバ通信網１０内のプライベートＩＰアドレスをキー情報としてＤＮＳサーバ７に個人の識別情報、有効期限、サービスカテゴリのユーザ情報を登録する。個人認証サーバ６は個人認証を正常に行ったことを認証サーバＧＷ１へ通知し、認証サーバＧＷ１はＮＡＴ機能５で使用するＮＡＴエントリ情報で個人認証状態を管理する。このようにして、ユーザの情報サーバ８へのアクセス可否を判定する。アクセス可であればユーザに情報サーバ８へのアクセスを許し、そうでなければユーザにアクセスを拒否したことを通知する。

【００４３】個人認証サーバ６は、個人認証を行いアクセスが許可されたことを端末３に通知する。端末３は個人認証サーバ６からの通知にしたがい、認証状態（認証中）を端末画面上に表示する。端末３は認証状態を定期的に個人認証サーバ６に問い合わせ、個人認証サーバ６がそれに応答することで端末３および個人認証サーバ６で連携して認証状態の相互確認を行う。個人認証サーバ６は端末３からの認証状態問い合わせにより、認証状態を継続し続ける。

【００４４】端末３から認証サーバ通信網１０内の情報サーバ８へのパケットは、宅内ＧＷ２で暗号カプセル化しＩＰｓｅｃトンネル４０を使用して認証サーバＧＷ１に送信する。このとき、暗号カプセル化しているパケットは、発アドレスは端末３の宅内通信網３０のプライベートアドレス、着アドレスは情報サーバ８の認証サーバ通信網１０内のプライベートＩＰアドレスである。認証サーバＧＷ１は、暗号カプセル化しているパケットを復号して取り出し、ＮＡＴ機能５の管理情報にしたがい、発アドレスを端末３の宅内通信網３０内のプライベートアドレスからユニークな認証サーバ通信網１０内のプライベートＩＰアドレスに付け替えを行い、情報サーバ８へパケットを送信する。

【００４５】情報サーバ８から端末３へのパケットは、認証サーバＧＷ１のＮＡＴ機能５で逆のアドレス付け替えを行い、認証サーバＧＷ１でパケットを暗号カプセル化して宅内ＧＷ２へ送信し、宅内ＧＷ２で復号してパケットを取り出し転送する。

【００４６】情報サーバ８は、ＤＮＳサーバ７にアクセスしてきた認証サーバ通信網１０内のプライベートＩＰアドレスをキーとしてＤＮＳサーバ７に問い合わせることでアクセスしてきたユーザの情報を取得する。

【００４７】端末３が情報サーバ８と個人認証状態を終了するとき、端末３から個人認証サーバ６に認証中状態の終了を要求する。個人認証サーバ６は、ＤＮＳサーバ７に対し認証状態を終了するユーザの情報をＤＮＳサーバ７から削除するため、削除要求を行う。このとき、個人認証サーバ６自身の個人認証状態をクリアする。また、個人認証サーバ６は、端末３からの認証状態問い合わせを監視し、一定期間認証状態問い合わせがないことを検出し認証状態の終了を行う。さらに、端末３が認証サーバ通信網１０内で使用していたプライベートＩＰアドレスのＮＡＴ情報はクリアされる。

【００４８】認証サーバ通信網１０内のプライベートＩＰアドレスを割り当てる手段として、端末３から最初のアクセスがあったときに認証サーバ通信網１０内のプライベートＩＰアドレスを割り当てる。

【００４９】個人認証未の場合の個人認証を促す手段として、端末３がＨＴＴＰ以外のプロトコルを使用している場合には、端末３に専用ＡＰＬを配備し端末３の専用ＡＰＬに個人認証を要求する。

【００５０】

【発明の効果】以上説明したように、本発明の第一の効果として、宅内ＧＷと認証サーバＧＷ間にＩＰｓｅｃトンネルを確立することにより、端末と情報サーバ間のセキュアな通信を可能とする。

【００５１】第二の効果は、認証サーバＧＷにＮＡＴ機能を具備することにより、グローバルＩＰアドレスが変わるダイアルアップ環境での宅内と認証サーバ通信網間のセキュアな通信を可能とする。

【００５２】第三の効果として、ＩＰレベル認証と個人認証の二段階による認証により、認証の強度を上げることを可能とする。

【００５３】第四の効果として、認証状態の開始または

11

終了に合わせてＤＮＳサーバへユーザ情報登録または削除を行うことにより、情報サーバはアクセスを受け付けた認証サーバ通信網内プライベートＩＰアドレスからユーザ情報の取得を可能とする。これによりユーザに対して、認証サーバ通信網１０内の複数のサービスを利用する際、その都度認証を行う必要がない、いわゆるＳＳＯサービスの提供を可能とする。

【００５４】第五の効果として、端末と個人認証サーバの連携により、端末が認証状態を把握することを可能とする。

【００５５】第六の効果として、端末と個人認証サーバの連携により、認証状態を維持することを可能する。

【００５６】第七の効果として、認証サーバＧＷのＮＡＴエントリ情報で個人認証状態を管理することにより、個人認証未の場合に個人認証を促すことを可能とする。

【００５７】第八の効果として、認証サーバ通信網内プライベートアドレスをキー情報としたＩＰレベル認証と個人認証の連携により、ＩＰレベル認証の対象と個人認証の対象を管理することを可能とする。

【図面の簡単な説明】

【図１】本発明実施例のインターネット中継接続方式の全体構成図。

12

＊【図２】宅内ＧＷと認証サーバＧＷとの間に確立されたＩＰｓｅｃトンネルの概念図。

【図３】異なるネットワーク間を転送されるパケットのアドレス付与状況を示す図。

【図４】個人認証サーバ、ＤＮＳサーバ、情報サーバ相互間の動作を示す図。

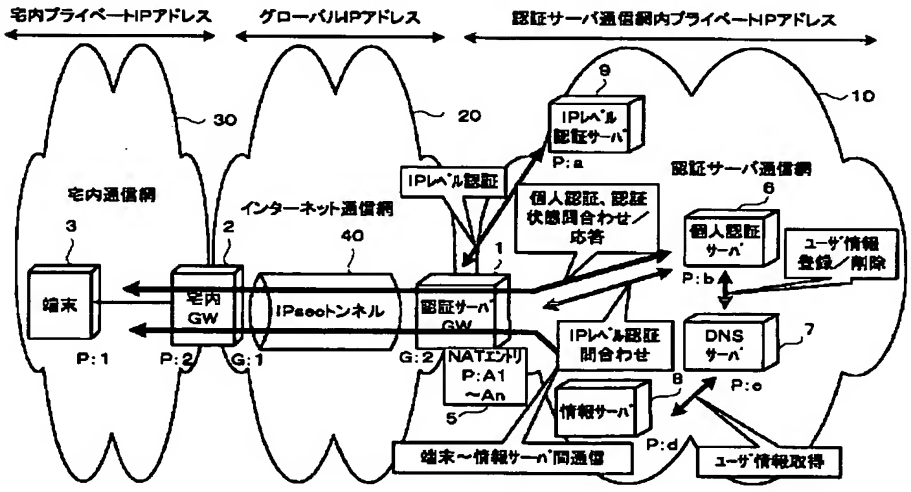
【図５】本発明実施例のインターネット中継接続方式の全体的な動作を示す図。

【符号の説明】

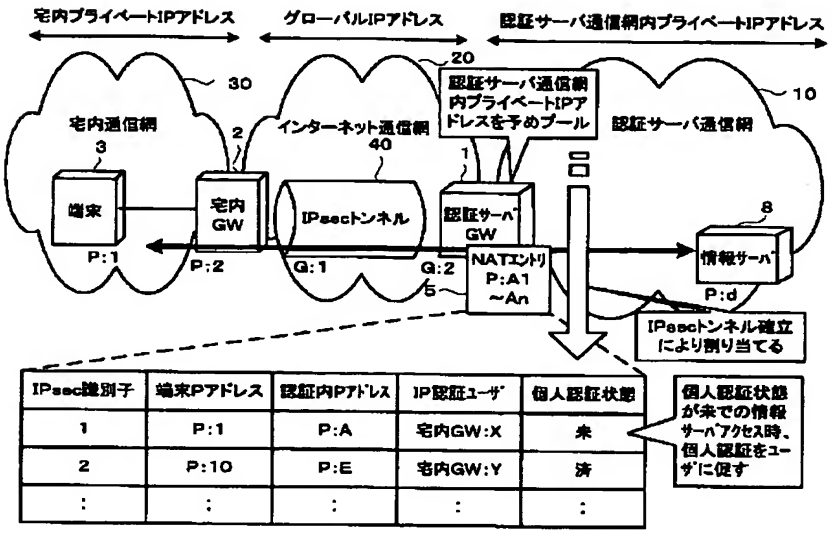
１　認証サーバＧＷ
２　宅内ＧＷ
３　端末
５　ＮＡＴ機能
６　個人認証サーバ
７　ＤＮＳサーバ
８　情報サーバ
９　ＩＰレベル認証サーバ
１０　認証サーバ通信網
２０　インターネット通信網
３０　宅内通信網
４０　ＩＰｓｅｃトンネル

＊

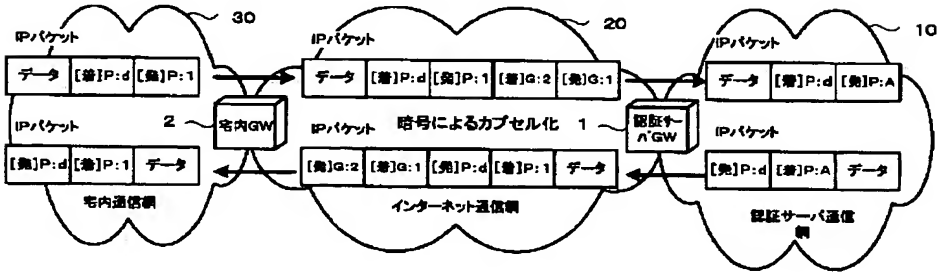
【図１】



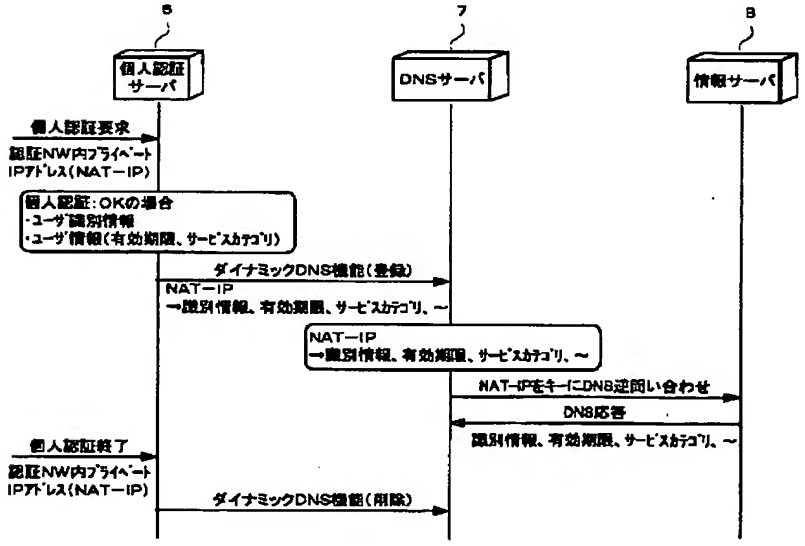
【図２】


宅内プライベートIPアドレス
グローバルIPアドレス
認証サーバ通信網内プライベートIPアドレス
30
宅内通信網
3
端末
P:1
2
宅内GW
P:2
20
認証サーバ通信網内プライベートIPアドレスを予めプール
インターネット通信網
40
IPsecトンネル
G:1
G:2
1
認証サーバGW
NATエントリ
P:A1
～An
5
10
認証サーバ通信網
8
情報サーバ
P:d
IPsecトンネル確立により割り当てる
IPsec識別子
端末IPアドレス
認証内IPアドレス
IP認証ユーザ
個人認証状態
1
P:1
P:A
宅内GW:X
未
2
P:10
P:E
宅内GW:Y
済
:
個人認証状態が未での情報サーバアクセス時、個人認証をユーザに促す

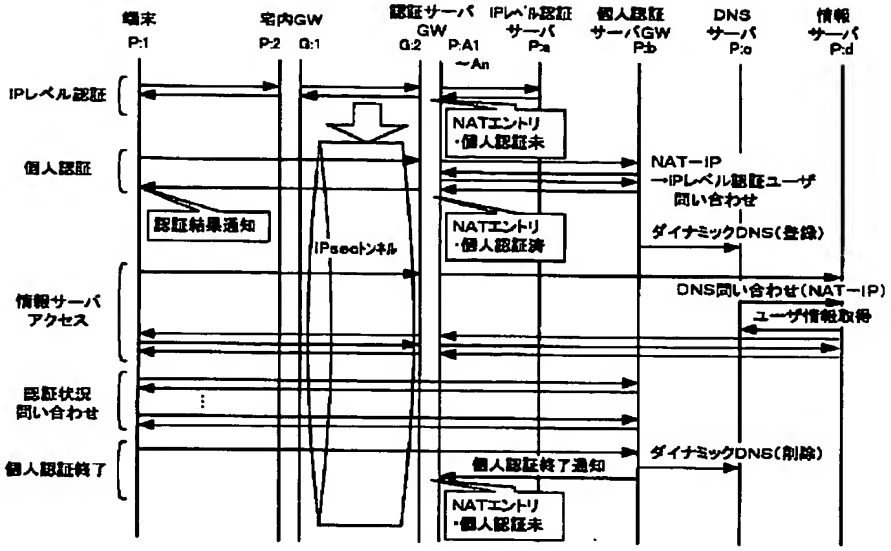
【図３】


30
IPパケット
データ
[着]P:d
[発]P:1
IPパケット
[発]P:d
[着]P:1
データ
2
宅内GW
宅内通信網
20
IPパケット
データ
[着]P:d
[発]P:1
[着]G:2
[発]G:1
IPパケット
暗号によるカプセル化
[発]G:2
[着]G:1
[発]P:d
[着]P:1
データ
1
認証サーバGW
インターネット通信網
10
IPパケット
データ
[着]P:d
[発]P:A
IPパケット
[発]P:d
[着]P:A
データ
認証サーバ通信網

【図４】


5
個人認証サーバ
7
DNSサーバ
8
情報サーバ
個人認証要求
認証NW内プライベートIPアドレス(NAT－IP)
個人認証：OKの場合
・ユーザ識別情報
・ユーザ情報(有効期限、サービスカテゴリ)
ダイナミックDNS機能(登録)
NAT－IP
→識別情報、有効期限、サービスカテゴリ、～
NAT－IP
→識別情報、有効期限、サービスカテゴリ、～
NAT－IPをキーにDNS逆問い合わせ
DNS応答
識別情報、有効期限、サービスカテゴリ、～
個人認証終了
認証NW内プライベートIPアドレス(NAT－IP)
ダイナミックDNS機能(削除)

【図５】



フロントページの続き

(72)発明者　井上　拓也
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

(72)発明者　溝口　陽一
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

Ｆターム(参考)　5B085 AE02 AE23 BG07
5B089 HA10 KA17 KC58
5J104 AA07 KA01 PA07
5K030 GA15 HA08 HB18 HC01 HC13
HD03 HD06 HD09 JL07 JT06
KA04 KA13 LA07 LB15 LD19